UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,348	10/19/2000	Bruce Leroy Beukema	AUS9-2000-0631-US1	6902

35525 7590 01/13/2006

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
SHIN, KYUNG H	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 01/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/692,348	BEUKEMA ET AL.	
	Examiner	Art Unit	
	Kyung H. Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application filed 10/19/2000.

2. Claims **1 - 25** are pending. Claims **1, 10, 12** have been amended. Independent claims are **1, 10, 12, 13, 22, 24, 25**.

Response to Arguments

3. Applicant's arguments filed **10/5/05** have been fully considered but they are not persuasive.

Response to Remarks

3.1 Applicant argues that the referenced prior art does not disclose *" ... motivation to also include a key as part of the message/packet, as transmitting a key along with the encrypted messages as taught by Williams would be effectively defeat the entire purpose of Williams ... " (see Remarks Page 8, Lines 12-14)*

The Williams (6,304,973) prior art discloses the capability to perform transparent security (i.e. key management, encryption/decryption) over a local area network environment (i.e. a subnet, a collection of network nodes). Once the security environment has been initialized, security procedures operate at network layer 3 and from a user standpoint network data packet transfers operate analogous to a normal TCP/IP network. (see Williams col. 21, lines 6-15: normal TCP/IP data communications after security parameter setup is completed) The Williams (6,304,973) prior art would not be concerned as to whether an access key parameter (i.e. or any other type of data) is transmitted over the network.

The Williams (6,304,973) and Frezza (4,638,356) prior art combination

discloses the capability to utilize a parameter (i.e. an access key), which is utilized to determine whether access is allowed or not allowed for a network node. (see Williams col. 5, lines 39-41: each network packet processed by security procedures ; see Frezza col. 2, lines 40-51; col. 2, lines 31-33; col. 3, line 65 - col. 4, line 4; col. 4, lines 10-15; col. 4, lines 25-28: access control utilizing an access (i.e. key) parameter)

The motivation for the combination of these two references would be obvious to one skilled in the art. The Williams (6,304,973) prior art would transparently transfer the access key parameter. The Williams (6,304,973) and Frezza (4,638,356) prior art combination discloses the capability to utilize an access key parameter in the determination of access to a network node or network environment (i.e. LAN) with router.

3.2 Applicant argues that the referenced prior art does not disclose " ... *the device that is private to a node and another device that is shared with a partition of a multi-partitioned network ...* " *(see Remarks Page 11, Lines 28-29)* ; " ... one of the devices is private to a node and the other is shared ... " (see Remarks Page 12, Lines 20-21)

The Williams (6,304,973) and Moiin (6,449,641) prior art combination discloses the capability for a shared and a non-shared configuration for disk devices storage within a clustered and a partitioned network environment. (see Moiin col. 2, lines 18-20; col. 13, lines 41-44: shared and non-shared configuration

; col. 4, lines 15-19; col. 4, lines 24-26: cluster membership ; col. 4, line 66 - col. 5, line 4: partitioned network environment)

3.3 Applicant argues that the referenced prior art does not disclose *" ... any type of subnet manager attached to a subnet that is responsible for configuring and managing switches, routers, and channel adapters of the subnet ... " (see Remarks Page 13, Lines 12-13)*

The Williams (6,304,973) prior art discloses a manager for a subnet. By definition, a subnet is defined as *" ... all the machines at one geographic location, in one building, or on the same local area network (LAN) ... "* . (1.http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213065,00.html) The Williams (6,304,973) prior art discloses security procedure operating over a local area network environment, which can also be a subnet environment. (see Williams col. 6, lines 46-51; col. 2, lines 25-29: secure local area network (i.e. a subnet environment))

The Williams (6,304,973) prior art discloses an administrator (i.e. subnet manager) for the NSC (Network Security Center), which controls and configures hosts (i.e. router can be a host, channel adapters within a host system) systems. The NSC performs the setup of the security parameters and network configuration. (see Williams col. 18, lines 6-19: local area network environment (i.e. subnet) administrator for secure environment (i.e. local area network))

3.4 Applicant argues that the referenced prior art does not disclose *" ... incrementing a counter when a key mismatch is encountered ... " (see Remarks Page 14, Line*

12)

The Williams (6,304,973) prior art discloses the capability to process network management events. (see Williams col. 17, lines 19-27: event processing) In addition, the Williams (6,304,973) and Kekic (56,664,978) prior art combination discloses the capability to utilize standard threshold parameter processing. Network Management techniques such as event monitoring, logging and event parameter update are obvious additions for management of network resources. This type of processing is well known in the art and is analogous to the invention's claim limitation of a counter (i.e. a threshold parameter) incremented in response to the occurrence of an event. The event processed is a mismatch between a first key and a second key (i.e. key mismatch). (see Williams col. 17, lines 19-27: event processing ; see Kekic col. 27, lines 12-18; col. 69, lines 58-59: threshold parameter (i.e. access key) mismatch, threshold parameter (i.e. access key, counter) update)

3.5 Applicant argues that Williams (6,304,973) and Frezza (4,638,356) prior art combination is a nonobvious combination and is not allowed.

The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Furthermore, in response to applicant's

arguments against the reference individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejection - 35 USC § 103

The text of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. **Claims 1 - 4, 7 - 16, 19 - 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Williams et al.** (US Patent No. 6,304,973) in view of **Frezza et al.** (US Patent No. 4,638,356) and further in view of **Moiin et al.** (US Patent No. 6,363,495).

Regarding Claims 1, Williams discloses a method in a node for managing authorized attempts to access the node, the method comprising:

d) storing, by the node information from the packet; (see Williams col. 17, lines 19-27: *During audit processing, information from the packet is stored.*)

e) sending, by the node the information to a selected recipient in response to a selected event. (see Williams col. 5, lines 39-41; col. 17, lines 19-27: *All Network accesses are monitored and selected event are audited. During the audit process a selected recipient is sent information concerning the audited event.*)

Williams discloses a secure network environment controlling access to distributed network nodes and event processing such as a threshold parameter mismatch. (see Williams col. 4, lines 28-33; col. 22, lines 48-52; col. 17, lines 19-27: *"... centralized administration of a layer 3 secure network ... distributed over the Internet ... provide a security device that prevents unauthorized third parties from gaining access to a host ... "*) In addition, Williams discloses receiving a network packet from a source and verifying an authorized IP address (see Williams col. 22, lines 48-52). But, Williams does not explicitly teach an authentication process with a node access key parameter in a network packet.

However, Frezza discloses in "Apparatus and Method for Restricting Access to a Communications Network", an authentication process that involves restricting access to a network with a node access key parameter, whereby the key is stored in the header of network packet. (see Frezza col. 6, lines 37-44) The key is used to determine whether it is valid to access a network resource (e.g. frame verifier, FV, codes), then if the items match, authentication is successful. (see Frezza col. 2, lines 40-51)

Frezza discloses:

c) dropping, by the node the packet without a response to the source if the first key does not match the second key; (see Frezza col. 2, lines 40-51; col. 2, lines 31-33; col. 3, line 65 - col. 4, line 4; col. 4, lines 10-15; col. 4, lines 25-28: access

control utilizing a parameter (i.e. an access key), network event management processing)

Williams-Frezza does not specifically disclose a partitioned network, however, Williams-Frezza in view of Moiin discloses a secure partitioned network utilizing shared devices. The applicant's invention discloses a partitioned network that enables access to shared devices. The two systems disclose partitioned networks utilizing shared devices, therefore, both systems are equivalent.

Frezza and Moiin disclose:

a) receiving, by the node a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node receiving the packet can determine which of the partitions of the multi-partitioned network can access the node receiving the packet; (see Frezza col. 6, lines 37-44; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes with a partitioned network, access to shared disk drives)

b) determining, by the node whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node; (see Frezza col. 2, lines 40-51; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes within a partitioned network, access to shared disk drives)

Network resource sharing techniques, which reduce operational costs due to a reduction in the total number of required network resources, are well known concepts for a network. A partitioned network enables network nodes to access shared network resources such as disk devices. Implementation of shared resources within a distributed network is an obvious and efficient addition to any network.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams with a network packet containing a key to determine whether it is valid as taught in Frezza, and to enable clustering techniques within a partitioned network as taught by Moiin. One would have been motivated to include a node key that is transmitted within the network packet by employing Frezza in order to have a strengthened authentication process by restricting access from unauthorized attempts on the network, and to employ Moiin in order to optimize configuration of a clustered partitioned network environment. (see Moiin col. 4, lines 40-43: *" ... each node has more complete information regarding the potential member nodes of the new cluster, the resulting new cluster consistently has a relatively optimal configuration ..."*)

Regarding Claims 2, 14, Williams discloses the method of claims 1 and 13, wherein the selected event is a request from the recipient for the information. (see Williams col. 5, lines 51-55; col. 18, lines 11-19: *Access violations, security related events, are reported to Network Security Controller (NSC) and are transmitted to audit process*

which is designated as a recipient)

Regarding Claims 3, 15, Williams discloses the method of claims 1 and 13, wherein the selected event is an occurrence of a trap. (see Williams col. 17, lines 19-27: *The occurrence of a trap, which is designated an interrupt on Page 23 of specification, initiates audit process. Exception events are audited.*)

Regarding Claims 4, 16, Williams discloses the method of claims 1 and 13, wherein the selected event is a periodic event. (see Williams col. 17, lines 19-27: *Audit process tracks events occurring at a periodic interval such as an exception event*)

Regarding Claims 7, 19, Williams discloses the method of claims 1 and 13, wherein the node comprises at least one device private to the node and at least one device shared with at least one of the partitions of the multi-partition network. (see Williams col. 27, lines 38-47: *Alternate embodiment modifies NSC to retrieve access key for a node from a principal such as a subnet manager. Subnet manager is a SAN device used to configure and manage devices. The partition key is transmitted from the subnet manager to the manager software for inclusion in the authentication process;* see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes with a partitioned network, access to shared disk drives)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams to enable clustering capabilities techniques

within a partitioned network as taught by Moiin. One would have been motivated to employ Moiin in order to optimize the configuration of a clustered partitioned network environment. (see Moiin col. 4, lines 40-43)

Regarding Claims 8, 11, 20, 23, Williams discloses the method of claims 1, 10, 13 and 22, wherein the information includes at least one of a source local identifier, a destination local identifier, the key value, a global identifier address. (see Williams col. 17, lines 19-27: *"... detailed information about the individual packets transmitted and received ... " Key values information in network packets is audited. The subnet manager transmits an identifier (source local, destination local, global identifier address) or a key value to the manager software for inclusion in the authentication process.*)

Regarding Claims 9, 21, Williams discloses the method of claims 7 and 13, wherein the selected recipient is a subnet manager attached to a subnet that is responsible for configuring and managing switches, routers and channel adapters of the subnet. (see Williams col. 17, lines 19-27; col. 27, lines 38-47: *Alternate embodiment modifies NSC to send audit information concerning access violations to principal such as a subnet manager. The network manager transmits the required information to the subnet manager controlling the SAN.*)

Regarding Claim 10, Williams discloses a method in a node for managing authorized attempts to access the node, the method comprising:

d) storing information from the packet; (see Williams col. 17, lines 19-27: *During audit processing, information from the packet is stored.*)

e) sending the information to a selected recipient in response to a selected event. (see Williams col. 5, lines 39-41; col. 17, lines 19-27: *All Network accesses are monitored and selected event are audited. During the audit process a selected recipient is sent information concerning the audited event.*)

Williams discloses a secure network environment controlling access to distributed network nodes and event processing such as a threshold parameter mismatch. (see Williams col. 4, lines 28-33; col. 22, lines 48-52; col. 17, lines 19-27: *"... centralized administration of a layer 3 secure network ... distributed over the Internet ... provide a security device that prevents unauthorized third parties from gaining access to a host ... "*) In addition, Williams discloses receiving a network packet from a source and verifying an authorized IP address (see Williams col. 22, lines 48-52). But, Williams does not explicitly teach an authentication process with a node access key parameter in a network packet.

However, Frezza discloses in "Apparatus and Method for Restricting Access to a Communications Network", an authentication process that involves restricting access to a network with a node access key, whereby the key is stored in the header of network packet. (see Frezza col. 6, lines 37-44) The key is used to determine whether it is valid to access a network resource (e.g. frame

verifier, FV, codes), then if the items match authentication is successful. (see Frezza col. 2, lines 40-51)

Frezza discloses:

c) dropping the packet without a response to the source if the first key does not match the second key; (see Frezza col. 2, lines 40-51; col. 2, lines 31-33; col. 3, line 65 - col. 4, line 4; col. 4, lines 10-15; col. 4, lines 25-28: access control utilizing a parameter (i.e. an access key), network event management processing)

Williams-Frezza does not specifically disclose a partitioned network, however, Williams-Frezza in view of Moiin discloses a secure partitioned network utilizing shared devices. The applicant's invention discloses a partitioned network that enables access to shared devices. The two systems disclose partitioned networks utilizing shared devices, therefore, both systems are equivalent.

Frezza and Moiin disclose:

a) receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node that received the packet can determine which of the partitions of the multi-partitioned network can access the node that received the packet; (see Frezza col. 6, lines 37-44; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col.

13, lines 41-44; col. 13, lines 52-55: network nodes with a partitioned network, access to shared disk drives)

b) determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node; (see Frezza col. 2, lines 40-51; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes within a partitioned network, access to shared disk drives)

Network resource sharing techniques, which reduce operational costs due to a reduction in the total number of required network resources, are well known concepts for a network. A partitioned network enables network nodes to access shared network resources such as disk devices. Implementation of shared resources within a distributed network is an obvious and efficient addition to any network.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams with a network packet containing a key to determine whether it is valid as taught in Frezza, and to enable clustering techniques within a partitioned network as taught by Moiin. One would have been motivated to include a node key that is transmitted within the network packet by employing Frezza in order to have a strengthened authentication process by restricting access from unauthorized attempts on the network, and to employ Moiin in order to optimize configuration of a clustered partitioned network environment. (see Moiin col. 4, lines 40-43)

Regarding Claim 12, Williams discloses a data processing system comprising:

a) a bus system; a channel adapter unit connected to a system area network fabric; a memory connected to the bus system, wherein the memory includes as set of instructions; (see Williams col. 18, lines 44-50) and

b) a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the data processing system can determine which of the partitions of the multi-partitioned network can access the data processing system; (same as 1.a); determine whether the first key matches a second key for the data processing system (same as 1.b); drop the packet without a response to the source if the first key does not match the second key (same as 1.c); store information from the packet (same as 1.d); and send the information to a selected recipient in response to a selected event. (same as 1.e) These limitations encompass the same scope of the invention as that of the claim 1.a - e, therefore these limitations are rejected for the same reason as the claim 1.a - e.

Regarding Claims 13, 22, 24, 25, Williams discloses a method in a node for managing authorized attempts to access the node and a node, the method comprising:

c) dropping the packet without a response to the source if the first key does not match the second key; (see Williams col. 22, lines 48-52: *Due to access violation (first key does not match second key) packet processing is stopped and no indication is returned to the source.*)

d) storing information from the packet; (see Williams col. 17, lines 19-27: *During audit processing, information from the packet is stored.*)

e) sending the information to a selected recipient in response to a selected event. (see Williams col. 5, lines 39-41; col. 17, lines 19-27: *All Network accesses are monitored and selected event are audited. During the audit process a selected recipient is sent information concerning the audited event.*)

Williams discloses a secure network environment controlling access to distributed network nodes. (see Williams col. 4, lines 28-33: *"... centralized administration of a layer 3 secure network ... distributed over the Internet ... provide a security device that prevents unauthorized third parties from gaining access to a host ... "*)

Network resource sharing techniques, which reduce operational costs due to a reduction in the total number of required network resources, are well known concepts for a network. A partitioned network enables network nodes to access shared network resources such as disk devices. Implementation of shared resources within a distributed network is an obvious and efficient addition to any network.

Williams-Frezza does not specifically disclose a partitioned network,

however, Williams-Frezza in view of Moiin discloses a secure partitioned network utilizing shared devices. The applicant's invention discloses a partitioned network that enables access to shared devices. The two systems disclose partitioned networks utilizing shared devices, therefore, both systems are equivalent.

a) receiving a packet from a source, wherein the packet includes a first key, wherein the first key is a partition key associated with a particular partition of a multi-partitioned network having a plurality of partitions, and is used such that the node can determine which of the partitions of the multi-partitioned network can access the node; (see Frezza col. 6, lines 37-44; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes with a partitioned network, access to shared disk drives)

b) determining whether the packet is from a partition authorized to access the node by determining whether the first key matches a second key for the node; (see Frezza col. 2, lines 40-51; see Moiin col. 4, lines 15-19; col. 4, line 66 - col. 5, line 4; col. 13, lines 41-44; col. 13, lines 52-55: network nodes within a partitioned network, access to shared disk drives)

Williams discloses receiving a packet from a source and verifying an authorized IP address (see Williams col. 22, lines 48-52), but does not explicitly teach an authentication process with a node key in packet. However, Frezza discloses in "Apparatus and Method for Restricting Access to a Communications Network", an authentication process that involves restricting access to a network

with a node key, whereby the key is stored in the header of network packet (see Frezza col. 6, lines 37-44) The key is used to determine whether it is valid to access a network resource (e.g. frame verifier, FV, codes), then if the items match authentication is successful. (see Frezza col. 2, lines 40-51)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams with a packet containing a key to determine whether it is valid as taught in Frezza, and to enable clustering techniques within a partitioned network as taught by Moiin. One would have been motivated to include a node key that is transmitted within the network packet by employing Frezza in order to have a strengthened authentication process by restricting access from unauthorized attempts on the network, and to employ Moiin in order to optimize configuration of a clustered partitioned network environment. (see Moiin col. 4, lines 40-43: "*... each node has more complete information regarding the potential member nodes of the new cluster, the resulting new cluster consistently has a relatively optimal configuration ...*")

5. **Claims 5, 6, 17, 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Williams-Frezza-Moiin** and further in view of **Kekic et al.** (US Patent No. 6,664,978).

Williams discloses a secure network environment controlling access to network nodes

distributed over the Internet. (see Williams col. 4, lines 28-33: *"... provide a centralized administration of a layer 3 secure network ... distributed over the Internet ... provide a security device that prevents unauthorized third parties from gaining access to a host ..."*) Network Management techniques such as event monitoring, logging and event parameter update are obvious additions for management of network resources. Williams does not specifically disclose updating a counter value at the occurrence of a monitored event (i.e. key mismatches) occurring, however, Kekic discloses a network management system monitoring events and updating a counter value for a monitored parameter (i.e. key mismatches) and performing a specific action when a pre-determined threshold is surpassed. The applicant's invention discloses the update of a counter of key mismatch events and a pre-determined action being performed when a threshold value is surpassed. The two systems disclose monitoring event occurrences and performing pre-determined actions when a threshold is surpassed, therefore both systems are equivalent.

Regarding Claim 5, 17, Kekic discloses the method of claim 1 and 13 further comprising: incrementing a counter source if the first key does not match the second key. (see Kekic col. 27, lines 12-18; col. 69, lines 58-59: counter value is updated when event (i.e. key mismatch) is encountered)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams to include the ability to update a count of key mismatches as taught by Kekic. One of ordinary skill in the art would be motivated to

enhance Williams in order to perform event driven network management activities. (see Kekic col. 4, line 66 - col. 5, line 4: *"... standards-based network management solution for computer networks having a computer network management capability. The managed element server of this invention efficiently manages a constantly changing and growing heterogeneous computer network ...")*

Regarding Claim 6, 18, Kekic discloses the method of claim 5 and 13, wherein the selected event occurs when the counter source exceeds a threshold value. (see Kekic col. 27, lines 12-18; col. 69, lines 58-59: counter value triggers a specific action when a threshold value is surpassed)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Williams to include the ability to update a key mismatches counter and perform a specific action when a threshold value is surpassed as taught by Kekic. One of ordinary skill in the art would be motivated to enhance Williams in order to perform event driven network management activities. (see Kekic col. 4, line 66 - col. 5, line 4)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
December 22, 2005

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100